Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
	)	
Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act	)	GN Docket No. 14-126

To: The Federal Communications Commission

Comment of the Federal Trade Commission

In its inquiry into the status of broadband availability and deployment to all Americans, the Federal Communications Commission has asked for comment regarding the relevance of privacy and/or data security concerns to consumer adoption of broadband.[1] Among other issues, the FCC asked whether broadband providers must comply with their own voluntary statements about privacy and security and whether any other potential obligations exist for providers.[2] As reflected in our enforcement, research, and policy work on consumer privacy issues, the FTC believes that promoting consumer trust in digital technology is of critical importance to

[1] Federal Communications Commission, *Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, GN Docket No. 14-126, Tenth Broadband Progress Notice of Inquiry, 29 FCC Rcd 9747 (rel. Aug. 5, 2014)("NOI").

[2] *Id.* at 9769 ¶ 47 ("If privacy and/or security statements are offered voluntarily, are there any obligations, contractual or otherwise, for broadband providers to comply with such commitments? Are there other obligations regarding privacy and/or security which broadband providers may be subject? If so, what are these, and what relevance, if any, would they have to our [section 706(b)] determination [as to whether advanced telecommunications capability is being deployed to all Americans in a reasonable and timely fashion]?").

consumers and businesses alike. The FTC therefore appreciates the opportunity to provide comment to the FCC on the privacy and security practices of broadband providers and their impact on broadband adoption.

I. Broadband Service Providers Must Comply with a Number of Consumer Privacy and Data Security Laws Enforced by the FTC

Many of the federal laws enforced by the FTC impose obligations on broadband service providers to protect the privacy and security of consumer data. These laws include the Federal Trade Commission Act[3] ("FTC Act"), the Fair Credit Reporting Act[4] ("FCRA"), and the Children's Online Privacy Protection Act[5] ("COPPA"). As discussed further below, these laws prohibit broadband operators from making deceptive claims in their representations to consumers about privacy and data security. Further, they impose a variety of other requirements that may apply to broadband providers engaging in certain activities.

A. Section 5 of the FTC Act

Section 5 of the FTC Act proscribes "deceptive" or "unfair" acts or practices in or affecting commerce.[6] A company acts deceptively if it makes materially misleading statements or omissions.[7] Such statements or omissions can be express or implied. A company engages in unfair acts or practices if its practices cause, or are likely to cause, substantial injury to consumers that is neither reasonably avoidable by consumers themselves nor outweighed by

[3] 15 U.S.C. §§ 41-58.

[4] 15 U.S.C. §§15 U.S.C. §1681-1681x.

[5] 15 U.S.C. §§ 6501-6506.

[6] 15 U.S.C. § 45.

[7] *See* Fed. Trade Comm'n, Policy Statement on Deception, appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

countervailing benefits to consumers or to competition.[8] Section 5's prohibition against deceptive or unfair practices plays an important role in protecting consumers: put simply, it requires companies to market their products truthfully and to refrain from engaging in harmful business practices. Section 5 also promotes competition on the basis of truthful claims and provides an incentive for companies to act responsibly and fairly in providing their products and services. Although Section 5 contains an exemption for 'common carrier' activities, this exemption does not apply to the provision of other services, even if offered by common carriers.[9] Broadband Internet access services are not currently offered on a common carrier basis,[10] and the FTC therefore has jurisdiction over such services.[11]

Accordingly, a broadband provider that makes commitments – either expressly or implicitly – regarding its privacy or security practices, and fails to live up to such commitments, risks violation of Section 5 of the FTC Act.[12] Moreover, even absent such statements, a

---

[8] *See* Fed. Trade Comm'n, Policy Statement on Unfairness, appended to *Int'l Harvester Co*., 104 F.T.C. 949, 1070 (1984).

[9] 15 U.S.C. §§ 44, 45(a)(2). *See FTC v. Verity Int'l, Ltd.*, 443 F.3d 48, 58-60 & n.4 (2d Cir. 2006) (citing, *inter alia*, *SW Bell Tel. Co. v. FCC*, 19 F.3d 1475, 1481 (D.C. Cir. 1994), and *Nat'l Ass'n of Reg. Util. Comm'rs v. FCC*, 533 F.3d 601, 608 (D.C. Cir. 1976)).

[10] *Verizon v. FCC*, 740 F.3d 623, 650 (D.C. Cir. 2014)); *Nat'l Cable Telecomm'ns Ass'n v. Brand X Internet Servs*., 545 U.S. 967, 993-95 (2005).

[11] The FCC's authority over non-common carrier broadband Internet access services pursuant to Title I of the Communications Act of 1934, 47 U.S.C. §§ 151-161, and Section 706 of the Telecommunications Act of 1996, 47 U.S.C. § 1302, has no bearing on the scope of the FTC's jurisdiction, since, under Sections 5(a) and 13(b) of the FTC Act, 15 U.S.C. §§ 45(a) & 53(b), "the FTC may proceed against unfair practices even if those practices [also] violate some other statute…." *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1195 (10th Cir. 2009) (referring to Telecommunications Act provision). *See also*, *FTC v. T-Mobile USA, Inc.*, No. 2:14-cv-00967 Docket No. 1 (W.D. Wa. July 1, 2014) (action against carrier for deceptive and unfair practices in violation of FTC Act in connection with placing third-party charges on telephone bills); Fed. Trade Comm'n Staff, *Broadband Connectivity Competition Policy* (2007), at 38-41 (analyzing the application of Section 5 of the FTC Act to broadband services), *available at* http://www.ftc.gov/sites/default/files/documents/reports/broadband-connectivity-competition-policy/v070000report.pdf.

[12] *See Broadband Connectivity Competition Policy*, *supra* note 11, at 130-136 (discussing potential deception and unfairness issues in the broadband Internet access service industry).

broadband provider that fails to reasonably protect the privacy or security of consumer data in a way that causes a likelihood of substantial harm that is not reasonably avoidable by consumers and is without countervailing benefits to consumers or competition may violate the unfairness prohibition of Section 5.

Indeed, the FTC has used Section 5 to challenge dozens of companies' express and implied claims about what data they collect, whether they share it with third parties, what choices they offer to consumers, and the level of security they provide for consumers' personal data. To date, the FTC has brought over 50 cases alleging lax security practices, 20 of which charged that the business had engaged in unfair acts or practices. The FTC's privacy and security matters have involved businesses in a wide variety of industries, including companies that sell mobile and Internet connected devices;[13] companies that provide Internet-related services;[14] social media companies;[15] and mobile app developers.[16] The FTC has also brought numerous cases against companies that it charged had interfered with or invaded consumer privacy by surreptitiously collecting data through software, including"spyware" and other

[13] *HTC America, Inc.*, Docket No. C-4406 (F.T.C. June 25, 2013) (final decision and order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf; *TRENDnet, Inc.*, Docket No. C-4426 (Jan. 16, 2014) (final decision and order), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.

[14] *Google, Inc.*, Docket No. C-4336 (F.T.C. Oct. 13, 2011) (final decision and order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.

[15] *Facebook, Inc.*, Docket No. C-4365 (F.T.C. Aug. 10, 2012) (final decision and order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

[16] *Snapchat, Inc.*, Matter No. 132-3078 (F.T.C. May 14, 2014) (proposed consent agreement), *available at* http://www.ftc.gov/system/files/documents/cases/140508snapchatanalysis.pdf; *United States v. Path, Inc.*, No. C-13-0448 (N.D. Cal. Feb. 8, 2013) (Stipulated Final J.), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.

malware installed on consumers' computers,[17] or by sending unwanted or deceptive "spam" emails[18] or text messages.[19]

B. Fair Credit Reporting Act

Another law that imposes privacy and security-related obligations on broadband providers is the FCRA. Although best known for regulating the activities of credit bureaus, the FCRA also applies to companies that provide information to credit bureaus ("furnishers") and companies that use credit reports ("users"). Broadband providers often are both furnishers and users under the FCRA.[20] As such, certain FCRA requirements apply. For example, if a broadband provider furnishes information to credit bureaus, the FCRA imposes obligations to make sure the information is accurate. If the provider uses credit reports, it must certify to the credit bureaus that it has a "permissible purpose" for obtaining the report, such as the fact that it will use the report to set credit or employment terms. A broadband provider that uses credit reports must also provide notices to its customers when it offers less favorable terms based on information in a credit report. These notices must explain how the consumer can dispute any inaccurate information in their credit report.

---

[17] *See, e.g., Aaron's, Inc.*, Docket No. C-4442 (Mar. 10, 2014) (final decision and order), *available at* http://www.ftc.gov/system/files/documents/cases/140311aaronsdo.pdf.

[18] *See, e.g., FTC v. Linda Jean Lightfoot d/b/a Universal Direct*, No. C-3-02-145 (S.D. Ohio Apr. 11, 2002) (stipulated preliminary injunction), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2002/04/lightfootstip.pdf.

[19] *See, e.g., FTC v. Advert Mktg., Inc.*, No. 4:13-cv-00590 (S.D. Tex. June 9, 2014) (Stipulated Final J.), *available at* http://www.ftc.gov/system/files/documents/cases/140612advertorder.pdf.

[20] The FCRA does not contain an exemption for common carrier services.

The FTC's recent enforcement action against Time Warner Cable illustrates this last requirement.[21] There, the FTC charged Time Warner Cable with obtaining prospective customers' credit reports before providing them with video, high-speed data, telephony, and other services. According to the complaint, when credit reports contained negative information, the company required consumers to pay a deposit or to pre-pay the first month's bill. The FTC alleged that Time Warner Cable, in violation of the FCRA, did so without providing a "risk-based pricing notice" to consumers. To settle these charges, Time Warner Cable agreed to pay $1.9 million in civil penalties and to submit to a permanent injunction that bars further violations of the FCRA.

C. Children's Online Privacy Protection Act

COPPA imposes privacy and security requirements on broadband providers to the extent their conduct or knowledge triggers the law's requirements. COPPA applies to both operators of child-directed websites and other online services that collect personal information from children and operators of general audience sites and other online services that knowingly collect personal information from children. Operators subject to COPPA must provide notice and obtain verifiable parental consent before they collect personal information from children under 13 years of age. COPPA defines "personal information" to include online contact information, persistent identifiers, geolocation information, and other types of identifiers. In addition to the parental notice and consent obligations, COPPA also requires covered operators to provide access to the data they collect, to establish security procedures, and imposes retention limits.

[21] *United States v. Time Warner Cable, Inc.*, No. 13 Civ. 8998 (S.D.N.Y. Dec. 20, 2013) (Stipulated Final J.) *available at* http://www.ftc.gov/sites/default/files/documents/cases/131219timewarnerstip.pdf.

The FTC has brought a number of cases to enforce these requirements against mobile app developers,[22] social media companies,[23] and others. To date, the FTC has brought 23 COPPA cases and obtained more than $9,000,000 in civil penalties. To the extent that a broadband service provider were to knowingly collect personal information from children under 13, it would be subject to COPPA's privacy and security requirements.

II. FTC Policy and Educational Efforts

In addition to the laws discussed above, the FTC has engaged in a variety of policy and education initiatives to promote privacy and data security in all sectors of the economy. This work provides important guidance that broadband providers can look to as they incorporate privacy and security best practices into their products and services.

A. Policy Initiatives

On the policy front, the FTC has hosted public workshops, issued reports, and frequently testified before Congress on business practices and technologies affecting the privacy and security of consumer data. For example, the FTC testified before Congress on privacy and data security related issues eight times in the last year.[24] The FTC's testimony detailed its efforts

---

[22] *See United States v. W3 Innovations, LLC.*, No. C-11-03958 (N.D. Cal. Sept. 8, 2011) (Stipulated Final J.), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/09/110908w3order.pdf.

[23] *See Path, Inc.*, *supra* note 16.

[24] *See* Prepared Statement of the Fed. Trade Comm'n, "*The Location Privacy Protection Act of 2014*," Before the Senate Committee on the Judiciary, 113th Cong., June 4, 2014, *available at* http://www.ftc.gov/system/files/documents/public_statements/313671/140604locationprivacyact.pdf; Prepared Statement of the Fed. Trade Comm'n, "*Emerging Threats in the Online Advertising Industry*," Before the Senate Committee on Homeland Security and Governmental Affairs, 113th Cong., May 15, 2014, *available at* http://www.ftc.gov/system/files/documents/public_statements/309891/140515emergingthreatsonline.pdf; Prepared Statement of the Fed. Trade Comm'n, "*Data Breach on the Rise: Protecting Personal Information from Harm*," Before the Senate Committee on Homeland Security and Governmental Affairs, 113th Cong., Apr. 2, 2014, *available at* http://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf; Prepared Statement of the Fed. Trade Comm'n, "*Protecting Personal Consumer Information from Cyber Attacks and Data Breaches*," Before the Senate Committee on Commerce, Science, and Transportation, 113th Cong., Mar. 26, 2014, *available at*

over the past decade to promote data security and privacy in the private sector through civil law enforcement, policy initiatives, and consumer and business education. In addition, the FTC testified about the privacy issues related to the data broker industry's collection and sale of consumer records and by the collection of consumer's precise geolocation data. The FTC also recently held workshops on the privacy and security implications of mobile device tracking[25] and the Internet of Things.[26] These workshops brought together various stakeholders to discuss the consumer benefits as well as the privacy and security risks associated with these new technologies. Such workshops allow the FTC to develop an important record of relevant issues and concerns as it develops guidance for industry best practices.

In 2007, the FTC issued a staff report, *Broadband Connectivity Competition Policy*, which, among other things discussed protecting consumers of residential broadband service. Specifically, the report found that "effective consumer protection in the broadband marketplace

---

http://www.ftc.gov/system/files/documents/public_statements/293861/140326datasecurity.pdf; Prepared Statement of the Fed. Trade Comm'n, "*Protecting Consumer Information: Can Data Breaches be Prevented?*" Before the House Committee on Energy and Commerce, 113th Cong., Feb. 5, 2013, *available at* http://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf; Prepared Statement of the Fed. Trade Comm'n, "*Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime*," Before the Senate Committee on the Judiciary, 113th Cong., Feb. 4, 2014, *available at* http://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-digital-age-preventing-data-breaches-combating/140204datasecuritycybercrime.pdf; Prepared Statement of the Fed. Trade Comm'n, "*Safeguarding Consumers' Financial Data*," Before the Senate Committee on Banking, Housing, & Urban Affairs, 113th Cong., Feb. 3, 2014, *available at* http://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-safeguarding-consumers-financial-data/140203financialdatasecurity.pdf; Prepared Statement of the Fed. Trade Comm'n, "*What Do Data Brokers Have on Consumers, And How Do They Use It?*" Before the Senate Committee on Commerce, Science, and Transportation, 113th Cong., Dec. 18, 2013, *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-entitled-what-information-do-data-brokers-have-consumers/131218databrokerstestimony.pdf.

[25] *See* Spring Privacy Series, *Mobile Device Tracking* (Feb. 19, 2014), *available at* http://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking.

[26] Fed. Trade Comm'n Workshop, *Internet of Things: Privacy & Security in a Connected World* (Nov. 19, 2013), *available at* http://www.ftc.gov/bcp/workshops/internet-of-things/.

will be essential to robust competition in that market," in part because "inadequate protection of privacy of personal information and data security in the provision of broadband Internet access could hamper consumer confidence in the industry."[27] The report concluded that the FTC and the FCC "each play[ ] an important role" in protecting consumers.[28] As for the FTC's role, the report also concluded that enforcement of the FTC Act, a flexible and effective tool, is critical to protecting consumers of broadband Internet access service.[29] These conclusions remain true today.

The FTC has also issued numerous reports on privacy issues. Over the years, it issued a report setting forth a general privacy framework for business,[30] a report on facial recognition technology,[31] a report on mobile privacy disclosures,[32] and a report on the data broker industry.[33] These reports have highlighted best practices that encompass a multi-faceted approach to protecting privacy and security.

---

[27] *Broadband Connectivity Competition Policy*, *supra* note 11, at 130.

[28] *Id*. at 161.

[29] *Id*. at 161-62.

[30] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[31] Fed. Trade Comm'n Staff, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies* (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

[32] Fed. Trade Comm'n Staff, *Mobile Privacy Disclosures: Building Trust Through Transparency* (2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

[33] Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability* (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Two points are worth noting in this regard. First, through its recent policy initiatives, the FTC has emphasized the importance of privacy by design.[34] While disclosure, as noted in the FCC's NOI, is an important element of a comprehensive approach to privacy and security, it does not guarantee adequate protections. For example, consumers should not have to sift through and compare disclosures to determine which companies implement which practices for the data they collect. Companies should simply implement practices that are reasonable given the context of the data collection. This is part of a privacy by design process that the FTC has encouraged all companies to implement.

Second, the FTC has set forth some best practices related to deep packet inspection ("DPI") and similar technologies.[35] In its 2012 Privacy Report, the FTC discussed the position of ISPs as major gateways to the Internet and their ability to access vast amounts of unencrypted data and to develop comprehensive profiles of their customers.[36]

B. FTC Consumer Education and Business Guidance

The FTC is also committed to promoting better privacy and data security practices through consumer education and business guidance. On the consumer education front, the FTC has distributed millions of copies of educational materials for consumers and businesses to address ongoing threats to security and privacy. It also makes its guidance materials available online. For example, the FTC recently released an updated version of "Net Cetera: Chatting with Kids About Being Online," a guide to help parents and other adults talk to kids about being safe,

---

[34] *See, e.g., Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 30, at 22. (Commissioner Ohlhausen and Commissioner Wright were not members of the FTC at the time and thus did not participate in the vote on the report.)

[35] DPI refers to an internet service provider's ("ISP") ability to analyze the information, comprised of data packets, that traverses its network when consumers use its service.

[36] *Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 30, at 55-56.

secure, and responsible online.[37] This new version deals with such topics as mobile apps and privacy, public Wi-Fi security, text message spam, and the amendments to the FTC's COPPA Rule. As another example, the FTC sponsors OnGuard Online, a website designed to educate consumers about basic computer security.[38] OnGuard Online and its Spanish-language counterpart, Alerta en Línea,[39] average more than 2.2 million unique visits per year. The FTC's website also includes timely advice to consumers on how to handle security breaches, such as the recent Target breach.[40]

Further, the FTC has released guidance directed to businesses. For instance, the FTC widely disseminates its business guide on data security,[41] along with an online tutorial based on the guide.[42] These resources provide a variety of businesses with practical, concrete advice as they develop data security programs and plans for their companies. This guidance provides an important resource for broadband providers, which often collect and maintain sensitive information about their customers.

---

[37] *See* http://www.consumer.ftc.gov/articles/pdf-0001-netcetera.pdf.

[38] *See* http://www.onguardonline.gov.

[39] *See* http://www.alertaenlinea.gov.

[40] *See* FTC Consumer Blog, *An Unfortunate Fact About Shopping* (Jan. 27, 2014), *available at* http://www.consumer.ftc.gov/blog/unfortunate-fact-about-shopping; FTC Consumer Blog, *Are you affected by the recent Target hack?* (Dec. 19, 2013), *available at* https://www.consumer.ftc.gov/blog/are-you-affected-recent-target-hack. In addition to these materials posted in response to recent breaches, the FTC has long published a victim recovery guide and other resources to explain the immediate steps identity theft victims should take to address the crime; how to obtain a free credit report and correct fraudulent information in credit reports; how to file a police report; and how to protect their personal information. *See* http://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[41] *See Protecting Personal Information: A Guide for Business, available at* http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.

[42] *See Protecting Personal Information: A Guide for Business (Interactive Tutorial), available at* http://business.ftc.gov/multimedia/videos/protecting-personal-information.

III. Conclusion

In sum, companies that provide broadband services must adhere to the privacy and security obligations imposed by the FTC Act, the FCRA, and COPPA. The FTC has actively enforced these laws and will continue to do so, where appropriate, in the broadband service market. As the FCC explores the laws and standards applicable to broadband providers, including those that may apply pursuant to the Communications Act, the FTC encourages the FCC to consider the well-established legal standards and best practices.[43] The FTC welcomes the opportunity to share its experience promoting consumer privacy and data security with the FCC and looks forward to working with the FCC to ensure a consistent, efficient, and effective approach to enforcement and oversight in the broadband area.

By Direction of the Federal Trade Commission, September 19, 2014

[43] *See Joint FCC/FTC Policy Statement for the Advertising of Dial-Around and Other Long-Distance Services to Consumers*, 15 FCC Rcd 8654, 8655-56 (2000) (discussing consistent substantive principles that FTC and FCC, respectively, apply to false or misleading advertising practices as "deceptive" under Section 5 of the FTC Act and "unjust and unreasonable" under Section 201(b) of the Communications Act).